

MCKOOL SMITH, P.C.
Robin L. Cohen (NJ Attorney ID No. 030501986)
Alexander M. Sugzda (*pro hac vice* application to be filed)
One Bryant Park, 47th Floor
New York, New York 10036
Tel: (212) 402-9400

Attorneys for Plaintiff FranConnect LLC

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

FRANCONNECT LLC,	:	Civil Action No.:
	:	2:19-CV-8408
	:	
Plaintiff,	:	
	:	
v.	:	
	:	<u>COMPLAINT</u>
	:	
FEDERAL INSURANCE COMPANY,	:	
	:	<u>JURY TRIAL DEMANDED</u>
Defendant.	:	
	:	
	:	

FranConnect LLC (“FranConnect”), with a principal place of business at 11800 Sunrise Valley Drive, Reston, VA 20191, by and through its undersigned attorneys, as and for its Complaint against Federal Insurance Company (“Federal”), with its principal place of business upon information and belief at 202B Hall’s Mill Road, Whitehouse Station, NJ 08889, alleges as follows:

PRELIMINARY STATEMENT

1. This action is for breach of contract, declaratory relief, breach of the implied covenant of good faith and fair dealing, and violation of the New Jersey

Consumer Fraud Act, arising out of Federal's unjustified refusal to provide coverage under an insurance policy it sold to FranConnect.

2. FranConnect is the named insured under Federal ForeFront Portfolio 3.0 Policy No. 8248-7480 (the "Policy"), which specifically provides coverage for losses resulting from "Computer Fraud" and "Funds Transfer Fraud."

3. FranConnect was the victim of a wire transfer fraud whereby the perpetrators of the fraud impersonated employees and principals of multiple entities, including Saratoga Investment Corp. ("Saratoga"), a lender to FranConnect. The perpetrators sent "spoofed" emails, purporting to be from specific individuals at Saratoga with whom FranConnect had regular contact, containing fraudulent wire transfer instructions. As a result, FranConnect sent a \$1,000,000 loan prepayment intended for Saratoga to an account controlled by the criminals. Virtually none of that money has been recovered (the "Loss").

4. The Policy FranConnect purchased is designed to protect FranConnect against precisely the type of loss it incurred as a result of the fraudulent wire transfer. Yet despite the fact that FranConnect paid its premiums, gave prompt notice of the Loss to Federal, and cooperated fully and completely with Federal's inquiry into the Loss, Federal has failed and refused

to pay FranConnect's claim for coverage under the Policy for the Loss (the "Claim"). This refusal to pay constitutes a breach of Federal's contractual obligations.

5. Federal has failed and refused to pay FranConnect's Claim despite the fact that it was recently ordered by the United States District Court for the Southern District of New York to provide coverage for an email spoofing fraud resulting in a fraudulent wire transfer under substantively identical policy language for "Computer Fraud" and "Funds Transfer Fraud" in *Medidata Solutions, Inc. v. Federal Insurance Co.*, 268 F. Supp. 3d 471 (S.D.N.Y. 2017), and that the *Medidata* trial court ruling was upheld on appeal by the United States Court of Appeals for the Second Circuit.

6. Federal's refusal to pay FranConnect's Claim is therefore not fairly debatable and constitutes a breach of the Policy's implied covenant of good faith and fair dealing.

7. Unfortunately, FranConnect is not the only policyholder to receive an unjustified denial of coverage from Federal for a loss caused by email spoofing under Federal policies purporting to cover "Computer Fraud" and/or "Funds Transfer Fraud." Email spoofing is targeting businesses and individuals with increasing frequency, and rather than provide coverage to its policyholders in the wake of such losses, Federal has engaged in a widespread pattern and practice of

denying email spoofing claims without adequate investigation or consideration under these coverages in a scheme to protect its own interests over those of its policyholders.

8. FranConnect seeks a declaration that there is coverage for the Claim under the Policy, damages for breach of contract due to Federal's unreasonable failure to honor its obligation under the Policy to cover the Claim, and damages for Federal's violation of the Policy's implied covenant of good faith and fair dealing as well as the New Jersey Consumer Fraud Act.

THE PARTIES

9. FranConnect is a limited liability company organized under the laws of Delaware, and maintains its principal place of business in Reston, Virginia. FranConnect is wholly owned by FranConnect Holdings, LLC ("Holdings"). There are two corporations that maintain an ownership interest in Holdings. The first is FranConnect Ultimate Holdings, Inc., a Delaware corporation with its principal place of business in California. The second is AMVA Holdings, Inc., a Delaware corporation with its principal place of business in Virginia. FranConnect distributes ownership interests in Holdings as compensation in the form of Management Incentive Units ("MIUs"). The individuals who maintain an ownership interest in the form of MIUs are residents of Virginia, Maryland, Florida, California, and Massachusetts. There are four persons who maintain an

outright ownership interest in Holdings, and not in the form of a MIU. These individuals are residents of Virginia and Florida.

10. Upon information and belief, Federal is an insurance company organized under the laws of the State of Indiana with its principal place of business in New Jersey. Upon information and belief, Federal is authorized to sell or write insurance in New Jersey and, at all material times, has conducted and continues to conduct substantial insurance business in the State of New Jersey, including engaging in the business of selling insurance, investigating claims, and/or issuing policies that cover policyholders or activities located in New Jersey.

JURISDICTION AND VENUE

11. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332 because there is complete diversity of citizenship between the parties to this action and because the amount in controversy exceeds \$75,000, exclusive of interest and costs.

12. Venue in this Court is proper pursuant to 28 U.S.C. § 1391.

FACTUAL ALLEGATIONS

I. The Federal Policy

13. In consideration of significant premiums paid to cover exactly the type of loss at issue here, Federal sold the Policy to FranConnect for the policy period March 31, 2018 to March 31, 2019.

14. The Policy provides coverage for a wide variety of criminal and fraudulent activity, including “Insuring Clause (E): Computer Fraud Coverage” and “Insuring Clause (F): Funds Transfer Fraud Coverage.”

15. The Policy provides “Limits of Liability” for its Computer Fraud Coverage and Funds Transfer Fraud Coverage of \$1,000,000, subject to a \$10,000 retention.

16. The Policy provides “Computer Fraud Coverage” for “direct loss of **Money, Securities or Property** sustained by an **Insured** resulting from **Computer Fraud** committed by a **Third Party**.”¹

17. **Money** is defined as “currency, coin, bank notes and bullion.”

18. **Third Party** is defined as “a natural person other than (A) an **Employee**; or (B) a natural person acting in collusion with an **Employee**.”

19. **Computer Fraud** is defined as: “[T]he unlawful taking of **Money, Securities or Property** resulting from a **Computer Violation**.”

20. **Computer Violation** includes both “an unauthorized (A) entry into or deletion of **Data** from a **Computer System**; [and] (B) change to **Data** elements or program logic of a **Computer System**, which is kept in machine readable format . . . directed solely against an **Organization**.”

¹ All emphasized terms appear in boldface in the Policy.

21. **Data** is defined as “information contained in records, manuscripts, accounts, microfilms, tapes or other records, which are processed and stored in a **Computer System**.”

22. The Policy defines “**Computer System**” as “a computer or network of computers, including its input, output, processing, storage and communication facilities, and shall include off-line media libraries.”

23. The Policy also provides “Funds Transfer Fraud Coverage” for “direct loss of **Money** or **Securities** sustained by an **Insured** resulting from **Funds Transfer Fraud** committed by a **Third Party**.”

24. **Funds Transfer Fraud** is defined as: “[F]raudulent written [or] electronic . . . instructions . . . purportedly issued by an **Organization**, and issued to a financial institution directing such institution to transfer, pay or deliver **Money** or **Securities** from any account maintained by such **Organization** at such institution, without such **Organization’s** knowledge or consent.”

25. The Policy also provides \$250,000 in Insuring Clause (J): Expense Coverage to FranConnect, subject to no retention. That provision provides:

(J) The Company shall pay the **Parent Organization** for:

(1) **Investigative Expenses** resulting from any direct loss covered under Insuring Clauses . . . (E), Computer Fraud Coverage; (F), Funds Transfer Fraud Coverage . . .

incurred by any **Organization** in the amount set forth in . . . the Crime Declarations, solely if such covered direct loss is in

excess of the Retention application to such covered loss. Such amount shall be part of and not in addition to the Limit of Liability applicable to such covered loss.

26. **Investigative Expenses** are defined in relevant part as “reasonable expenses . . . incurred by an **Organization** with the Company’s prior written consent to establish the existence and amount of a covered loss.”

II. **FranConnect Is the Victim of an Email Spoofing Fraud**

27. FranConnect provides management software to franchisors to help them better and more efficiently manage their franchise systems.

28. One of FranConnect’s sources of debt financing is Saratoga.

29. In May 2018, one or more criminals appear to have gained access to the email accounts of FranConnect, FranConnect’s majority shareholder Serent Capital (“Serent”), and/or Saratoga, and spoofed the email accounts of Mike Flecker, FranConnect’s chief financial officer, Charles Phillips, Managing Director and Portfolio Manager at Saratoga, Nick Martino, a Principal at Saratoga, Jeff Bolte, an Associate at Saratoga, John Caselli, Vice President of Serent, and Archith Murali, an Associate at Serent.

30. The criminals created spoofed email accounts for all of the above individuals by changing one letter in the email domain names. For example, “franconnect” was spoofed as “franconnact.”

31. When a recipient received a spoofed email, it appeared exactly as if it had been sent by the real sender, with the real sender's actual email address in the "From" line, even though it had been sent by the criminals. The change to the email address to reflect the spoofed email account was not apparent to the recipient when reading the spoofed email. The change to the spoofed email addresses was only noticeable if the recipient took the time to read every letter of the email address in the "To" line when he responded to the spoofed email, because it would be sent to the spoofed account controlled by the criminals.

32. The criminals used these spoofed email accounts to effectively hijack an email chain between those individuals discussing a \$1 million loan prepayment FranConnect was going to make to Saratoga.

33. On May 10, 2018, Mr. Flecker sent an email to Mr. Phillips and Mr. Martino, stating FranConnect would be making the \$1 million prepayment and requesting wire instructions for the payment.

34. The criminals then hijacked the email conversation, making sure genuine emails from the Saratoga and Serent members of the conversation went to the spoofed account they created for Mr. Flecker, and sending spoofed emails to Mr. Flecker appearing to be from the individuals at Serent and Saratoga.

35. On May 11, 2018, a spoofed email that appeared to come from Mr. Martino was sent to Mr. Flecker, attaching wire transfer instructions for the prepayment directing that it go to an account at Amegy Bank in Houston, Texas.

36. Upon information and belief, the Amegy Bank account is not a Saratoga account, and Mr. Martino did not send the email with the wire instructions.

37. That same day, due to the manipulations of the criminals, the actual wire instructions sent by Mr. Bolte at Saratoga instead appear to have gone to a spoofed email account for Mr. Flecker controlled by the criminals.

38. Mr. Flecker confirmed receipt of the wire instructions to who he believed was Mr. Martino, but was in fact one of the criminals, and directed FranConnect Controller Mohammad Shabbir to prepare the wire from FranConnect's account at East West Bank to the bank account provided by the criminals.

39. FranConnect then wired \$1,000,000 to the Amegy Bank account in the name of CEI Holdings, Inc., specified in the wire instructions sent by the criminals.

40. Mr. Flecker then confirmed to the criminals posing as Mr. Martino that the wire was sent, and the criminals sent an email purporting to be from Mr. Flecker to the real Mr. Martino saying the wire was being processed.

41. On May 14, 2018, the real Mr. Bolte sent an email to the real Mr. Flecker following up about the prepayment and providing correct wire instructions for Saratoga.

42. The criminals quickly worked to unwind this development and sent an email purporting to be from Mr. Martino to the real Mr. Bolte saying Saratoga had already received the funds, and an email purporting to be from Mr. Bolte to the real Mr. Flecker apologizing for the “misunderstanding” that the funds had not been received by Saratoga and confirming receipt of the funds in the Amegy Bank account.

43. The criminals, again pretending to be Mr. Bolte, thereafter asked for and received a wire confirmation from FranConnect’s bank system.

44. On July 10, 2018, the real Mr. Bolte contacted Mr. Shabbir to follow up for a confirmation of the prepayment wire and the fraud was discovered when Mr. Shabbir sent the confirmation showing the transfer to the CEI Holdings account at Amegy Bank account and Mr. Bolte replied that he was not familiar with that account information.

45. FranConnect thereafter hired the law firm DLA Piper to perform investigative work regarding the fraud and notified Federal of that retention. Amounts paid by FranConnect to DLA Piper and firms hired by DLA Piper are in excess of \$80,000.

46. Following discovery of the fraud, FranConnect was able to recover \$3,700.01 that remained in the Amegy Bank account, but despite working with law enforcement, it has not been able to recover the \$996,299.99 balance of the \$1,000,000 it transferred on May 11, 2018.

III. Federal's Denial of Coverage

47. On July 11, 2018, FranConnect promptly notified Federal of the fraudulent wire and made the Claim for coverage under the Policy.

48. Federal acknowledged receipt of the Claim and requested certain information from FranConnect, all of which FranConnect provided to the extent possible.

49. Coverage exists under the Computer Fraud Coverage because by altering the "From" line of the spoofed emails used in the fraud to make them appear as if they came from the real individuals at FranConnect, Saratoga, and Serent's email accounts, the criminals committed an unauthorized entry of information into FranConnect's computer system (the use of the email addresses of the spoofed individuals) as well as the unauthorized deletion of information from FranConnect's computer system (the criminals' actual email addresses). The change of the email address in the "From" line from the criminals' actual email address to the spoofed individuals' email addresses was also an unauthorized change to information in FranConnect's computer system. Thus, there was a

Computer Violation, and because that **Computer Violation** resulted in an unlawful taking of **Money**, there was **Computer Fraud**.

50. Coverage also exists under the Funds Transfer Fraud Coverage. Once Mr. Flecker believed that the emails from the criminals were really from the individuals at Saratoga based on the altered “From” line, Mr. Flecker, Mr. Shabbir, and any other FranConnect employees involved in wiring the funds became unwitting participants in the fraud and expressed the instructions of the perpetrators of the fraud, not FranConnect. Fraudulent electronic instructions were sent to a financial institution, East West Bank, to wire funds to the Amegy Bank account specified by the criminals. Because FranConnect never intended to send the \$1 million prepayment meant for its lender to a bank account controlled by criminals it had no knowledge of, the funds were not wired with FranConnect’s knowledge or consent. Thus, there was a **Funds Transfer Fraud**.

51. Despite this, on November 20, 2018, Federal denied coverage for the Claim, stating that coverage was not available under the Computer Fraud Coverage or the Policy’s separate Social Engineering Fraud Coverage.

52. In the November 20 letter, Federal stated it could not “identify any other relevant insuring clauses that may apply,” and did not even discuss coverage under the Policy’s Funds Transfer Fraud Coverage.

53. On December 20, 2018, FranConnect disputed Federal's denial of coverage for the Claim and explained the reasons why the Claim was covered, including that Federal had recently been ordered by the United States District Court for the Southern District of New York to provide coverage under virtually identical policy language for a virtually identical loss, a ruling that had been affirmed by the United States Court of Appeals for the Second Circuit.

54. Despite these arguments, Federal maintained its denial of coverage under the Computer Fraud Coverage and also stated it was denying coverage under the Funds Transfer Fraud Coverage in a letter dated February 1, 2019.

55. The February 1 letter noted immaterial distinctions between FranConnect's Claim and the claim at issue in the *Medidata* case, and also showed lack of familiarity with FranConnect's claim by claiming FranConnect cited other authority, and attempting to distinguish that authority, despite the fact that FranConnect did not cite any authority other than *Medidata* in its December 20 letter.

56. By denying coverage when the Claim was covered under the Policy and all prerequisites to coverage were met, Federal breached its contractual obligation to FranConnect.

57. By denying coverage for a Claim in virtually identical circumstances under which it had already been ordered by at least one court to

provide coverage, Federal denied coverage for a Claim that was not fairly debatable, and thereby breached the Policy's implied covenant of good faith and fair dealing.

58. Upon information and belief, Federal has similarly denied coverage under computer fraud or funds transfer fraud coverage provisions in several other claims based on email spoofing, thereby forcing each of those policyholders to litigate against Federal to obtain coverage from individual courts that Federal has already been ordered to provide by one court. This is a quintessential breach of the Policy's implied covenant of good faith and fair dealing and constitutes a violation of the New Jersey Consumer Fraud Act.

FIRST CAUSE OF ACTION

(Breach of Contract)

59. Plaintiff repeats and realleges the allegations set forth in paragraphs 1 through 58 of this Complaint as if fully set forth herein.

60. The Policy constitutes a valid and enforceable contract between Federal and FranConnect because FranConnect was the named insured under the Policy.

61. FranConnect has paid all premiums, provided prompt notice of the claim, and otherwise performed all obligations required of it under the Policy.

62. Under the terms of the Policy, Federal must pay up to \$1,000,000 for a direct loss of **Money** that comes within the Policy definitions of **Computer Fraud** or **Funds Transfer Fraud**.

63. As detailed above, the facts of the Claim come within those Policy provisions.

64. Federal has not paid any amounts to FranConnect in connection with the Claim. By failing to provide coverage for the Claim, Federal has breached the terms of the Policy.

65. As a direct and proximate result of Federal's breach of the Policy, FranConnect has suffered damages in an amount to be determined at trial, plus consequential damages, attorneys' fees, and pre- and post-judgment interest to the extent permitted by law.

SECOND CAUSE OF ACTION

(Declaratory Relief)

66. Plaintiff repeats and realleges the allegations set forth in paragraphs 1 through 65 of this Complaint as if fully set forth herein.

67. Pursuant to the terms of the Policy, Federal is obligated to pay, up to the \$1,000,000 limit of liability, for a direct loss of **Money** that comes within the Policy definitions of **Computer Fraud** or **Funds Transfer Fraud**.

68. As detailed above, the facts of the Claim come within those Policy provisions.

69. Federal disputes its legal obligation to pay the Claim.

70. Pursuant to 28 U.S.C. § 2201, FranConnect is entitled to a declaration by this Court of Federal's obligations under the Policy.

71. An actionable and justiciable controversy exists between FranConnect and Federal concerning the proper construction of the Policy, and the rights and obligations of the parties thereto, with respect to the Claim for the fraudulent wire transfer.

72. FranConnect is entitled to a declaration declaring that there is coverage available for the Loss under the Policy, and, pursuant to 28 U.S.C. § 2202, any other relief this Court deems proper.

THIRD CAUSE OF ACTION

(Breach of the Implied Covenant of Good Faith and Fair Dealing)

73. Plaintiff repeats and realleges the allegations set forth in paragraphs 1 through 72 of this Complaint as if fully set forth herein.

74. There is an implied covenant of good faith and fair dealing in every insurance contract. This covenant obligates each party to the contract to refrain from taking any action or litigation position that would deprive the other of the benefits of the contract or cause undue hardship or harm to the other party. It also

requires the insurer to investigate claims in good faith and to reasonably and promptly pay covered claims.

75. FranConnect has paid all premiums, provided prompt notice of the claim, and otherwise performed all obligations required of it under the Policy.

76. By wrongfully denying coverage for the Claim, Federal breached the Policy, causing damages, including consequential damages.

77. Federal breached its duty to deal fairly and in good faith by engaging in conduct calculated to further its own economic interests at the expense of FranConnect.

78. This conduct includes denying coverage that it had already been ordered to provide for a virtually identical claim, as part of a pattern and practice of attempting to avoid coverage for claims based on email spoofing by rote denial without careful investigation and analysis of claims.

79. Federal recklessly disregarded these facts and denied payment to FranConnect to protect its own financial interests.

80. Federal has no fairly debatable basis to deny coverage to FranConnect. Federal's actions were in bad faith.

81. As a result of the foregoing, Federal is liable to FranConnect for compensatory, consequential, and punitive damages in an amount FranConnect may prove at trial.

FOURTH CAUSE OF ACTION

(Violation of New Jersey Consumer Fraud Act)

82. Plaintiff repeats and realleges the allegations set forth in paragraphs 1 through 81 of this Complaint as if fully set forth herein.

83. Federal is a person within the meaning of the New Jersey Consumer Fraud Act.

84. Federal sold the Policy to FranConnect and that action falls under the scope of the New Jersey Consumer Fraud Act.

85. All of Federal's actions and/or inactions in its performance under the Policy were in violation of the New Jersey Consumer Fraud Act.

86. Federal was deceptive in the adjustment of this Claim; in failing to pay any amounts owed under the Claim; in failing to timely pay the Claim; in scheming to defraud its policyholder; in acting in reckless disregard for its obligations under the Policy; in accepting premiums without the intention to pay monies owed for covered losses; in fraudulently telling its policyholder that the losses were not covered despite evidence that they were; in unilaterally denying covered losses without proper investigation; and in falsely misrepresenting what its responsibilities were under the Policy.

87. The above actions on the part of Federal were part of an ongoing, widespread, and continuous scheme to defraud its insureds in the payment of benefits under their policies of insurance.

88. FranConnect's experience is not an isolated case. The acts and omissions of Federal committed in this case, or similar acts and omissions, occur with such frequency that they constitute a general business practice of Federal with regard to handling these types of claims. Federal's process is unfairly designed to reach favorable outcomes for Federal at the expense of its policyholders. Specifically, Federal received a benefit when it refused to pay FranConnect's Claim because it retained hundreds of thousands of dollars that should rightfully have been paid to FranConnect under the Policy.

89. As a result of all of the above, Federal is in violation of the New Jersey Consumer Fraud Act and FranConnect seeks damages under the Act.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief as follows:

(a) On the First Cause of Action, Plaintiff requests that the Court enter judgment against Federal, awarding Plaintiff damages in an amount to be determined at trial but no less than \$996,299.99, plus consequential damages, attorneys' fees, and pre- and post-judgment interest to the extent permitted by law;

(b) On the Second Cause of Action, Plaintiff requests that this Court enter a declaratory judgment in favor of FranConnect against Federal, declaring that Federal is obligated to pay FranConnect, up to the applicable limits of the Policy, for the Claim;

(c) On the Third Cause of Action, Plaintiff requests that this Court enter judgment against Federal, awarding Plaintiff damages in an amount to be determined at trial;

(d) On the Fourth Cause of Action, Plaintiff requests that this Court enter judgment against Federal, awarding Plaintiff damages in an amount to be determined at trial; and

(e) Additionally, Plaintiff requests such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: March 12, 2019
New York, New York

MCKOOL SMITH, P.C.

By: /s/ Robin L. Cohen
Robin L. Cohen (NJ Attorney ID No.
030501986)

Alexander M. Sugzda (*pro hac vice*
application to be filed)

One Bryant Park, 47th Floor
New York, New York 10036

Tel: (212) 402-9400

rcohen@mckoolsmith.com

asugzda@mckoolsmith.com

*Attorneys for Plaintiff FranConnect
LLC*

LOCAL RULE 11.2 CERTIFICATION

Pursuant to Local Civil Rule 11.2, I certify under penalty of perjury that the matter in controversy alleged in the foregoing Complaint is not the subject of any other action pending in any court, or of any pending arbitration or administrative proceeding.

Dated: March 12, 2019
New York, New York

By: /s/ Robin L. Cohen
Robin L. Cohen (NJ Attorney ID No.
030501986)

One Bryant Park, 47th Floor
New York, New York 10036
Tel: (212) 402-9400
rcohen@mckoolsmith.com